****

**המחלקה להנדסת מערכות מידע ותכנה**

אבטחת מחשבים ורשתות תקשורת

(372-1-4601)

עבודה 4

תאריך ההגשה – 21.06.2019

הוראות כלליות:

* יש להעלות לאתר ה- Moodle קובץ מכווץ בשם ID1\_ID2 (ת"ז המגישים) המכיל קובץ Word או PDF.
* יש להעלות את העבודה לאתר המודל **ממשתמש אחד בלבד**.
* שאלות על העבודה יש לשאול **אך ורק** בפורום העבודות במודל, שאלות אשר ישאלו בדוא"ל לא יענו!
* יש לכתוב תשובות מלאות ומפורטות.
* כחלק מתהליך בדיקת העבודה תתבצע בדיקה לזיהוי עבודות מועתקות – **אל תעתיקו.** כל מקרה של העתקה יטופל על ידי ועדת משמעת אוניברסיטאית.

**שאלה 1 –** אנטי וירוסים **(20 נקודות)**

1. אנטי וירוס
   1. **(5 נקודות)** הסבירו את הקונספט של אנטי וירוס. מטרותיו, תחום אחריותו ואת מידת האינטרקציה הנדרשת ממנו עם המשתמש.
   2. **(5 נקודות)** מדוע התחום של Malware Analysis קיים ולא ניתן להסתפק באנטי וירוסים?
   3. **(5 נקודות)** הסבר מה הוא Virus Total? מתי כדאי להשתמש בו? בחר קובץ כלשהו חשוד ובדוק מה התוצאות המסופקות ע"י Virus Total. צרף את פלט התוכנית באמצעות תצלום מסך.
   4. **(5 נקודות)** הסבירו את ההבדל בין וירוסים ל-Malware.

**שאלה 2 –**  Malware Analysis **(20 נקודות)**

1. **(3 נקודות)** תארו את כללי האצבע הנדרשים בעת ביצוע Malware Analysis.
2. **(5 נקודות)** הסבירו את ההבדלים בין Static ו-Dynamic Analysis.
3. **(2 נקודות)** Strings2 בודק קבצים חשודים ושולח אותם לבדיקה ב-Virus Total? נכון/ לא נכון? הסבירו.
4. **(5 נקודות)** הסבר את התוכנה Procmon ומהי הדרך המומלצת לעבוד איתה?
5. **(5 נקודות)** ציינו את היתרונות והחסרונות של הכלי Cuckoo.

**שאלה 3 –** התקפות **(40 נקודות)**

1. **(10 נקודות)** תאר בפירוט ארבע דרכים שונות להזדהות מול מערכת (ספקו דוגמה מעשית לכל אחת מן הדרכים).
2. **(10 נקודות)** תאר את ההתקפות הבאות וכיצד ניתן להתגבר עליהן:
   1. Amplification Attacks
   2. Reflection Attacks
   3. SYN Spoofing Attack
3. **(10 נקודות)** הסבר מהו Buffer Overflow ותארו כיצד ניתן למנוע בזמן ריצה ובזמן ההידור.
4. **(10 נקודות)** נתונה מערכת מידע הכוללת טבלת משתמשים אשר בה העמודות Username ו-Password. הניחו כי למערכת ממשק הדורש הזדהות מול שני ערכים אלה.
   1. **(5 נקודות)** תארו התקפה אשר תאפשר למשתמש להזדהות ללא ידיעת שם המשתמש והסיסמה.
   2. **(5 נקודות)** תארו בפירוט כיצד ניתן למנוע את ההתקפה.

**שאלה 4 – חומות אש (20 נקודות)**

1. **(5 נקודות)** הסבר את ההבדל בין State-less Packet Filter ל- State-full Packet Filter. בתשובתך ציין יתרונות וחסרונות לכל אחד מהם.
2. **(15 נקודות)** אחרי ההצלחה המסחררת של סטטיק ובן-אל תבורי בארץ ובחו"ל התרחשו תקיפות סייבר רבות על הרשת הארגונית של מותגם.

למותג "סטטיק ובן אל תבורי" ישנן מספר מחלקות אשר לכל אחת מהן מספר שרתים:

* מחלקת קשרי החוץ (נמצאת בתת הרשת FRN) – למחלקה שרת HTTP בכתובת FR\_WEB.
* מחלקת הכספים (נמצאת בתת הרשת FN) – למחלקה שרת FTP פסיבי בכתובת FN\_FTP.

בנוסף, למותג המצליח ישנם שרת SMTP ושרת HTTP בכתובות SBT\_MAIL ו-SBT\_WEB המשמשים את המותג וגורמים חיצוניים (מעריצים, סוכנים, כותבי שירים, כוראוגרפים וכ"ו).

ישנו גם שרת TELNET בכתובת SBT\_TELNET.

כל השרתים פועלים בפורטים הסטנדרטיים של הפרוטוקול על גבי TCP:

HTTP – פורט 80, FTP – פורט 21, SSH – פורט 22, SMTP מוצפן – פורט 587, SMTP לא מוצפן – פורט 25, Storage – פורט 23

סטטיק ובן-אל הגדירו את המדיניות הבאה:

* שרת ה FTP של מחלקת הכספים יהיה זמין רק בתת הרשת FN.
* שרת ה HTTP של מחלקת קשרי החוץ חייב להיות זמין לכולם באינטרנט עבור בקשות HTTP מסוג GET ו POST. בקשות HTTP אחרות (למשל DELETE) מותרות רק עבור רק עבור מחשבים ברשת FRN.
* שרת ה - HTTP של המועדון צריך להיות זמין לכולם באינטרנט.
* שרת ה – SMTP של המותג צריך להיות זמין לכולם באינטרנט בשירות המוצפן שלו ולכלל הרשת גם בשירות הלא מוצפן שלו.
* שרת ה-TELNET יהיה זמין לכולם בארגון ולא ניתן לגישה מחוץ לארגון.
* כל השאר אסור.

למותג יש צורך בקניית חומות אש מסוג stateless packet filter הפועל ברמת ה Transport ולא מבצע deep packet inspection או מסוג Proxy server אשר פועל ברמת ה Application (עבור פרוטוקול מסוים בלבד).

סטטיק ובן-אל ביקשו את עזרתכם ביישום מדיניות האבטחה ברשת. שימו לב שעקב הוצאות חריגות על בגדים מכונפים וקעקועים של בן אל ותקציב עיצוב השיער הגבוה של סטטיק, ביקשו הלקוחות הנכבדים להפחית את מספר חומות האש שיצטרכו לרכוש למינימום האפשרי. כמו כן רכישת חומת אש מסוג Proxy server היא יקרה מאוד, ולכן יש לתת עדיפות ל stateless packet filters

1. תכננו והכינו תרשים של מבנה הרשת הארגונית ואת חומות האש הנחוצות. על התרשים לציין במפורש מהי כל תת רשת, את מיקום השרתים ואת מיקום חומות האש וסוגן.
2. עבור כל חומת אש מסוג stateless packet filter מלאו את טבלת החוקים שלה עפ"י הטבלה שהוצגה בתרגול.
3. עבור כל חומת אש מסוג Proxy server ציינו מדוע היה צורך דווקא בחומת אש מסוג זה ולא ניתן להסתפק ב-Stateless.